



US009141779B2

(12) **United States Patent**
Shen et al.

(10) **Patent No.:** **US 9,141,779 B2**
(45) **Date of Patent:** **Sep. 22, 2015**

(54) **USABLE SECURITY OF ONLINE PASSWORD MANAGEMENT WITH SENSOR-BASED AUTHENTICATION**

(75) Inventors: **Guobin Shen**, Beijing (CN); **Fan Yang**, Beijing (CN); **Lidong Zhou**, Beijing (CN)

(73) Assignee: **Microsoft Technology Licensing, LLC**, Redmond, WA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 296 days.

(21) Appl. No.: **13/110,939**

(22) Filed: **May 19, 2011**

(65) **Prior Publication Data**

US 2012/0297190 A1 Nov. 22, 2012

(51) **Int. Cl.**

G06F 21/00 (2013.01)

G06F 21/32 (2013.01)

H04L 9/32 (2006.01)

H04L 9/08 (2006.01)

H04L 29/06 (2006.01)

(52) **U.S. Cl.**

CPC **G06F 21/32** (2013.01); **H04L 9/0866** (2013.01); **H04L 9/32** (2013.01); **H04L 9/3231** (2013.01); **H04L 9/3271** (2013.01); **H04L 63/0861** (2013.01); **H04L 2209/805** (2013.01); **H04L 2463/082** (2013.01)

(58) **Field of Classification Search**

CPC **H04L 9/32**; **G06F 21/32**

USPC **726/5**

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,689,638 A 11/1997 Sadovsky
6,720,860 B1 4/2004 Narayanaswami

2001/0047488 A1 11/2001 Verplaetse et al.
2002/0038426 A1* 3/2002 Pettersson et al. 713/186
2003/0135740 A1 7/2003 Talmor et al.
2003/0158815 A1 8/2003 Yoshida et al.
2004/0192256 A1 9/2004 Kuwajima
2004/0205176 A1* 10/2004 Ting et al. 709/223
2004/0230826 A1 11/2004 Birkhoelzer et al.
2004/0249961 A1 12/2004 Katsube et al.
2005/0138385 A1 6/2005 Friedli et al.

(Continued)

OTHER PUBLICATIONS

Englert et al., "On the Design and Implementation of a secure Online Password Vault", Aug. 2009, pp. 375-382.*

(Continued)

Primary Examiner — Taghi Arani

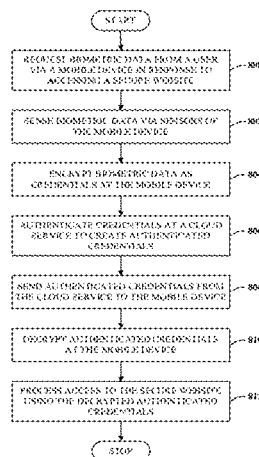
Assistant Examiner — Thaddeus Plecha

(74) *Attorney, Agent, or Firm* — Dan Choi; Judy Yee; Micky Minhas

(57) **ABSTRACT**

A multi-party security protocol that incorporates biometric-based authentication and withstands attacks against any single party (e.g., mobile phone, cloud, or the user). The protocol involves the function split between mobile and cloud and the mechanisms to chain-hold the secrets. A key generation mechanisms binds secrets to a specific device or URL (uniform resource locator) by adding salt to a master credential. An inline CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) handling mechanism uses the same sensor modality as the authentication process, which not only improves the usability, but also facilitates the authentication process. This architecture further enhances existing overall system security (e.g., handling untrusted or compromised cloud service, phone being lost, impersonation, etc.) and also improves the usability by automatically handling the CAPTCHA.

20 Claims, 13 Drawing Sheets



(56)

References Cited

U.S. PATENT DOCUMENTS

2006/0242415	A1 *	10/2006	Gaylor	713/176
2006/0279732	A1	12/2006	Wang et al.	
2007/0026372	A1 *	2/2007	Huelsbergen	434/322
2007/0143824	A1	6/2007	Shahazi	
2007/0186106	A1	8/2007	Ting et al.	
2007/0282757	A1 *	12/2007	Pandya et al.	705/76
2007/0293194	A1	12/2007	Bisht	
2007/0297610	A1	12/2007	Chen et al.	
2007/0300307	A1	12/2007	Duncan	
2008/0059804	A1 *	3/2008	Shah et al.	713/186
2009/0164795	A1	6/2009	Justus et al.	
2009/0205035	A1 *	8/2009	Sermersheim et al.	726/9
2009/0217056	A1 *	8/2009	Malpani	713/193
2009/0309698	A1 *	12/2009	Headley et al.	340/5.52
2010/0037046	A1 *	2/2010	Ferg et al.	713/155
2010/0049526	A1	2/2010	Lewis et al.	
2010/0115291	A1 *	5/2010	Buer	713/192
2010/0153722	A1 *	6/2010	Bauchot et al.	713/168
2010/0161927	A1 *	6/2010	Sprouse et al.	711/163
2011/0093942	A1 *	4/2011	Koster et al.	726/7
2011/0252243	A1 *	10/2011	Brouwer et al.	713/189
2011/0283338	A1	11/2011	Yang	
2011/0314533	A1 *	12/2011	Austin et al.	726/9

OTHER PUBLICATIONS

Pocovnicu, Adrian, "Biometric Security for Cell Phones", Retrieved at <<<http://revistaie.ase.ro/content/49/006%20-%20Pocovnicu.pdf>>>, Informatics Economical vol. 13, 2009.

Lu, et al., "M-Commerce Secured Using Web-enabled Mobile Biometric Agents", Retrieved at <<<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=4427633>>>, In the Proceedings of International Conferences on Web Intelligence and Intelligent Agent Technology, 2007.

Gamboa, et al., "Webbiometrics: User Verification Via web Interaction", Retrieved at <<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.4481&rep=rep1&type=pdf>>>, Sep. 11-13, 2007.

"Biometric Authentication for iPhone Apps", Retrieved at <<<http://www.securityweek.com/biometric-authentication-iphone-apps>>>, Security Week News, Aug. 3, 2010.

"Facer Credentialme™ Enables Biometric Authentication to Secure App for Smart Phone Security", Retrieved at <<<http://www.findbiometrics.com/industry-news/i/8638>>>, Feb. 14, 2011.

"Biometric authentication as a Service (BaaS)", Retrieved at <<<http://www.bioid.com/assets/files/Flyer/Flyer-BaaS-201103-EN-vFINAL-SCREEN.pdf>>>, Retrieved Date: Mar. 4, 2011.

"Windows Azure Platform", Retrieved at <<<http://www.microsoft.com/azure/>>>, Retrieved Date: Mar. 1, 2011.

"Clipperz", Retrieved at <<<http://www.clipperz.com/>>>, Retrieved Date: Mar. 1, 2011.

"LastPass", Retrieved at <<<http://lastpass.com/>>>, Retrieved Date: Feb. 28, 2011.

"OAuth Core ID", Retrieved at <<<http://oauth.net/core/1.0/>>>, Dec. 4, 2007.

"OpenID Specifications", Retrieved at <<<http://openid.net/developers/specs>>>, Retrieved Date: Feb. 28, 2011.

"SSL Man in the Middle Proxy", Retrieved at <<<http://crypto.stanford.edu/ssl-mitm/>>>, Retrieved Date: Feb. 28, 2011.

Adams, et al., "Users are not the Enemy", Retrieved at <<<http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/1999/p40-adams.pdf>>>, Communications of the ACM, vol. 42, Issue 12, Dec. 1999.

"Amazon Elastic Compute Cloud (Amazon EC2)", Retrieved at <<<http://aws.amazon.com/ec2/>>>, Retrieved Date: Feb. 28, 2011.

Aviv, et al., "Smudge Attacks on Smartphone Touch Screens", Retrieved at <<http://www.usenix.org/event/woot10/tech/full_papers/Aviv.pdf>>, In the Proceedings of the 4th USENIX conference on Offensive technologies, 2010.

Corner, et al., "Zero-interaction Authentication", Retrieved at <<<http://www.net-security.org/dl/articles/zia.pdf>>>, In the Proceed-

ings of the 8th annual international conference on Mobile computing and networking, Sep. 23-28, 2002.

Schneier, Bruce, "Password Safe Application", Retrieved at <<<http://www.schneier.com/passsafe.html>>>, Retrieved Date: Mar. 1, 2011.

Gouda, et al., "SPP: An Anti-phishing Single Password Protocol", Retrieved at <<<http://www.cse.msu.edu/~alexliu/publications/Password/sppjournal.pdf>>>, In the Proceedings of International Journal of Computer and Telecommunications Networking, vol. 51, Issue 13, Sep. 2007.

Griffin, Joel, "Study: U.S. Consumers would Welcome Voice Verification", Retrieved at <<<http://www.securityinfowatch.com/Financial/study-us-consumers-would-welcome-voice-verification>>>, Feb. 6, 2009.

Halderman, et al., "A Convenient Method for Securely Managing Passwords", Retrieved at <<<http://www.cse.umich.edu/~jhalderm/pub/papers/password-www05.pdf>>>, In the Proceedings of the 14th international conference on World Wide Web, May 10-14, 2005.

"Voiceverified", Retrieved at <<<http://www.voiceverified.com/>>>, Retrieved Date: Feb. 28, 2011.

Inglesant, et al., "The True Cost of Unusable Password Policies: Password Use in the Wild", Retrieved at <<<http://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf>>>, In the Proceedings of the 28th international conference on Human factors in computing systems, Apr. 10-15, 2010.

Kelsey, et al., "Secure Applications of Low-entropy Keys", Retrieved at <<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.4590&rep=rep1&type=pdf>>>, In the Proceedings of the First International Workshop on Information Security, 2007.

Kinnunen, et al., "Real-time Speaker Identification and Verification", Retrieved at <<http://cs.joensuu.fi/pages/tkinnu/webpage/pdf/IEEETrans06_Realtime.pdf>>, In the Proceedings of IEEE Transactions on Audio, Speech, and Language Processing, Jan. 2006.

Liu, et al., "uWave: Accelerometer-based Personalized Gesture Recognition and its Applications", Retrieved at <<<http://www.ruf.ie.edu/~mobile/publications/liu09percom.pdf>>>, 2009.

Manber, Udi, "A Simple Scheme to Make Passwords based on One-way Functions much Harder to Crack", Retrieved at <<<http://webglimpse.net/pubs/TR94-34.pdf>>>, 1996.

Abadi, et al., "Strengthening Passwords", Retrieved at <<<http://www.hpl.hp.com/techreports/Compaq-DEC/SRC-TN-1997-033.pdf>>>, Sep. 4, 2007.

Stanley, Morgan, "Mobile Ramping Faster than Desktop Internet did and will be Bigger than Most Think", Retrieved at <<http://www.morganstanley.com/institutional/techresearch/pdfs/Theme_2_Mobile_Ramping.pdf>>, Dec. 15, 2009.

"Fennec", Retrieved at <<<http://wiki.mozilla.org/Fennec>>>, Retrieved Date: Mar. 1, 2011.

Vance, Ashlee, "The New York Times", Retrieved at <<<http://www.nytimes.com/2010/01/21/technology/21password.html?scp=1&sq=passwords&st=cse>>>, Jan. 20, 2010.

Ross, et al., "Stronger Password Authentication using Browser Extensions", Retrieved at <<<http://crypto.stanford.edu/PwdHash/pwdhash.pdf>>>, In the Proceedings of the 14th conference on USENIX Security Symposium, vol. 14.

Sasse, et al., "Usable Security: Why do we need it? How do we get it?", Retrieved at <<http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec1extra/sasse_flechaiss_ch02.pdf>>, Aug. 5, 2005.

"Password Manager", Retrieved at <<http://en.wikipedia.org/wiki/Password_manager>>, Retrieved Date: Mar. 1, 2011.

"WebKit", Retrieved at <<<http://en.wikipedia.org/wiki/WebKit>>>, Retrieved Date: Mar. 1, 2011.

Saroiu, et al., "I am a Sensor, and I Approve this Message", Retrieved at <<<http://research.microsoft.com/en-us/um/people/ssaroiu/publications/hotmobile/2010/tenor.pdf>>>, In the Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications Feb. 22-23, 2010.

Bowman, et al., "Sensor based condition monitoring", Retrieved at <<http://www.bridge-project.eu/data/File/BRIDGE_WP03_sensor_based_condition_monitoring.pdf>>, Jun. 2009.

Diana, A, "Smartphones To Ring Up 28% of Holiday Shopping", InformationWeek, Nov. 22, 2010, 2 pages.

Ives B., et al., "The domino effect of password reuse", Commun. ACM 47, 4, Apr. 2004, pp. 75-78.

(56)

References Cited

OTHER PUBLICATIONS

"Non-Final Office Action," Mailed May 11, 2012, From U.S. Appl. No. 12/780,584, 26 pages.

"Response to Non-Final Office Action Mailed May 11, 2012," filed Aug. 9, 2012, From U.S. Appl. No. 12/780,584, 13 pages.

"Final Office Action," Mailed Jan. 4, 2013, From U.S. Appl. No. 12/780,584, 9 pages.

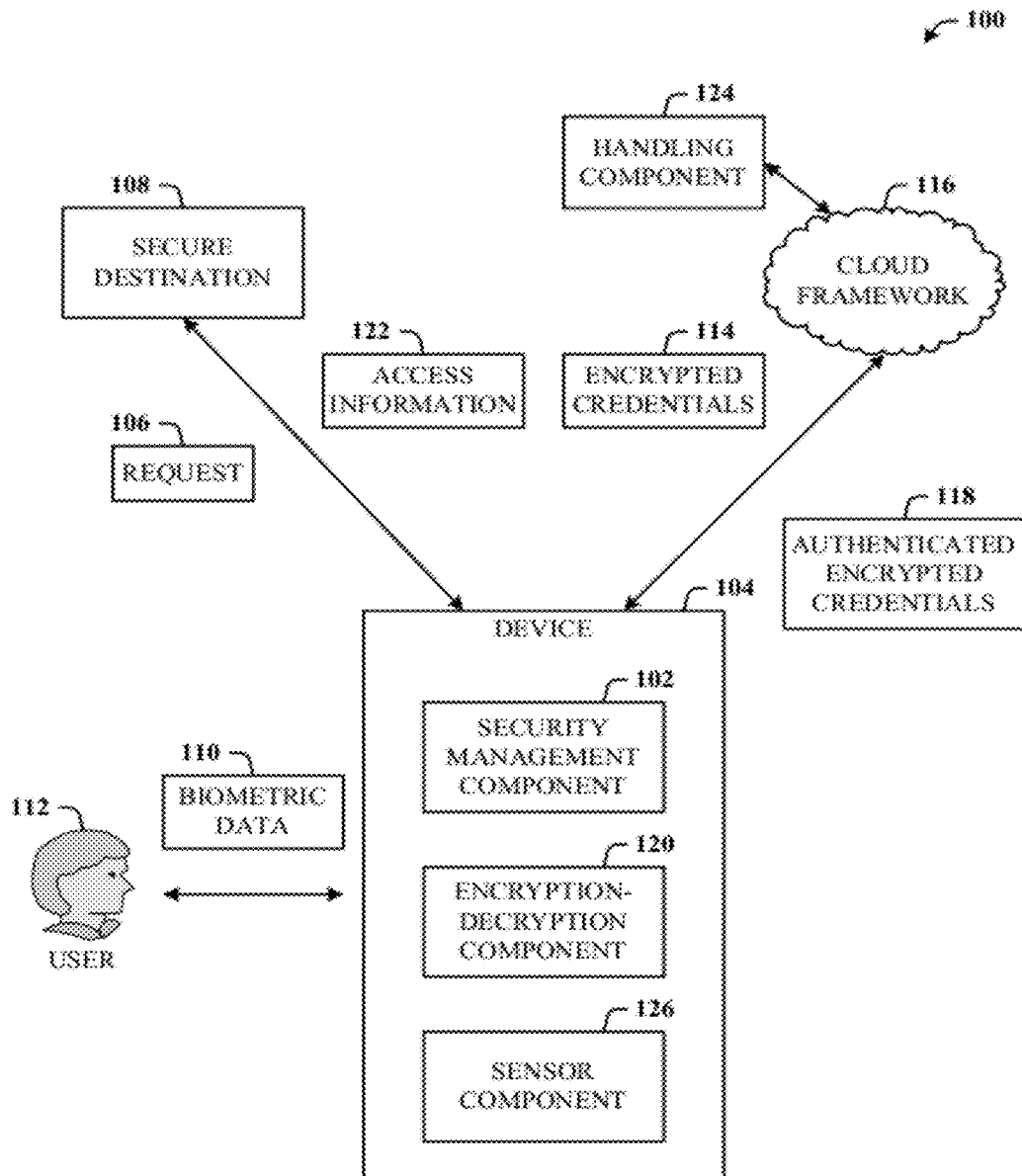
"Response to Final Office Action Mailed Jan. 4, 2013," filed Jan. 9, 2013, From U.S. Appl. No. 12/780,584, 12 pages.

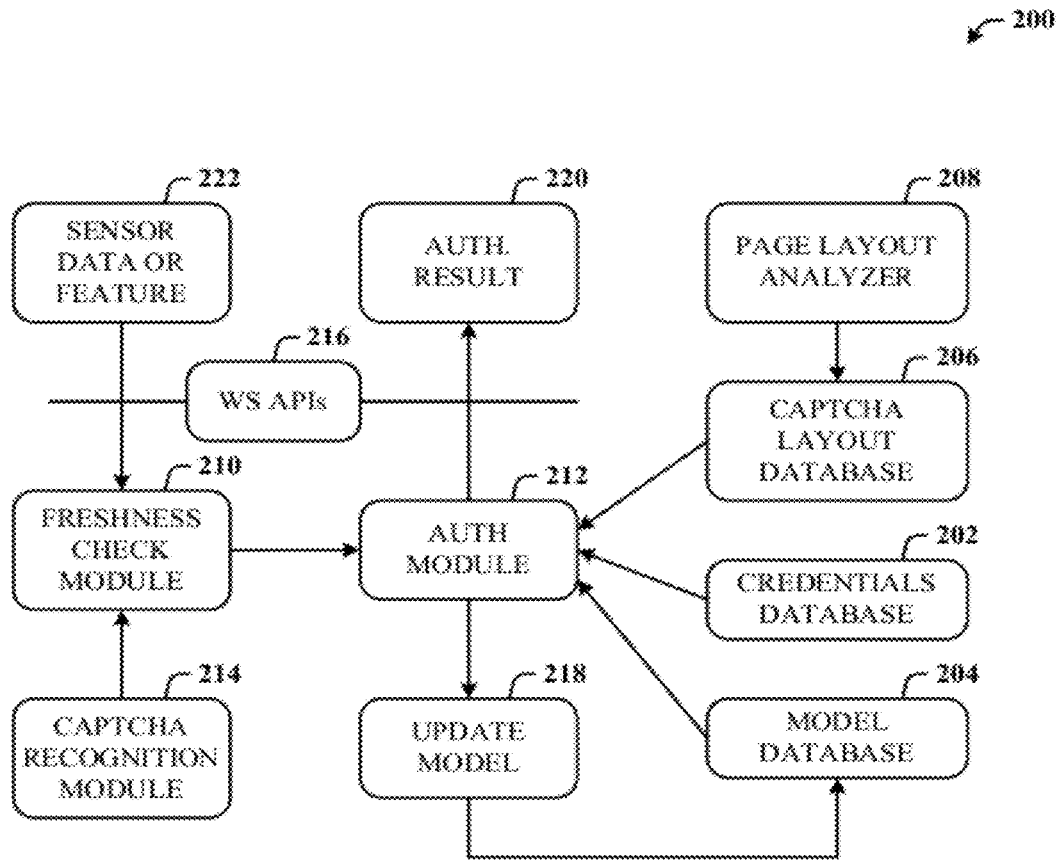
"Non-Final Office Action," Mailed Feb. 5, 2013, From U.S. Appl. No. 12/780,584, 9 pages.

"Response to Non-Final Office Action Mailed Feb. 5, 2013," filed Feb. 27, 2013, From U.S. Appl. No. 12/780,584, 11 pages.

"Notice of Allowance," Mailed Jul. 24, 2013, From U.S. Appl. No. 12/780,584, 9 pages.

* cited by examiner

**FIG. 1**

**FIG. 2**

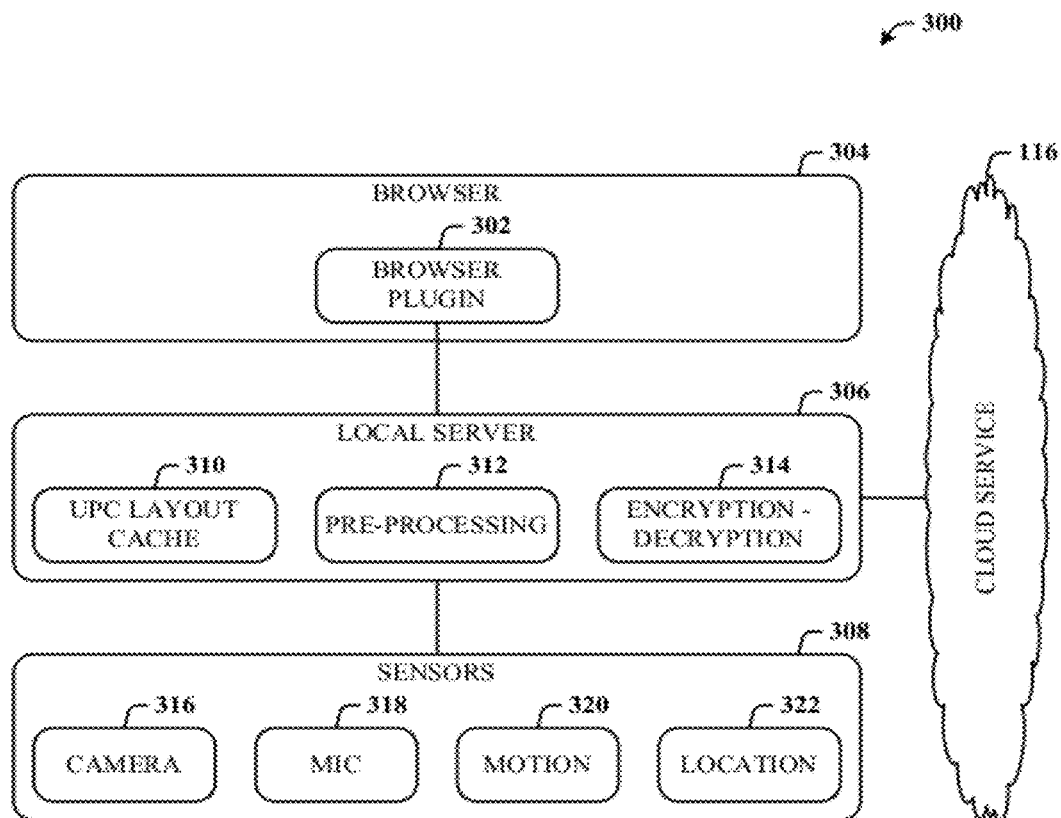
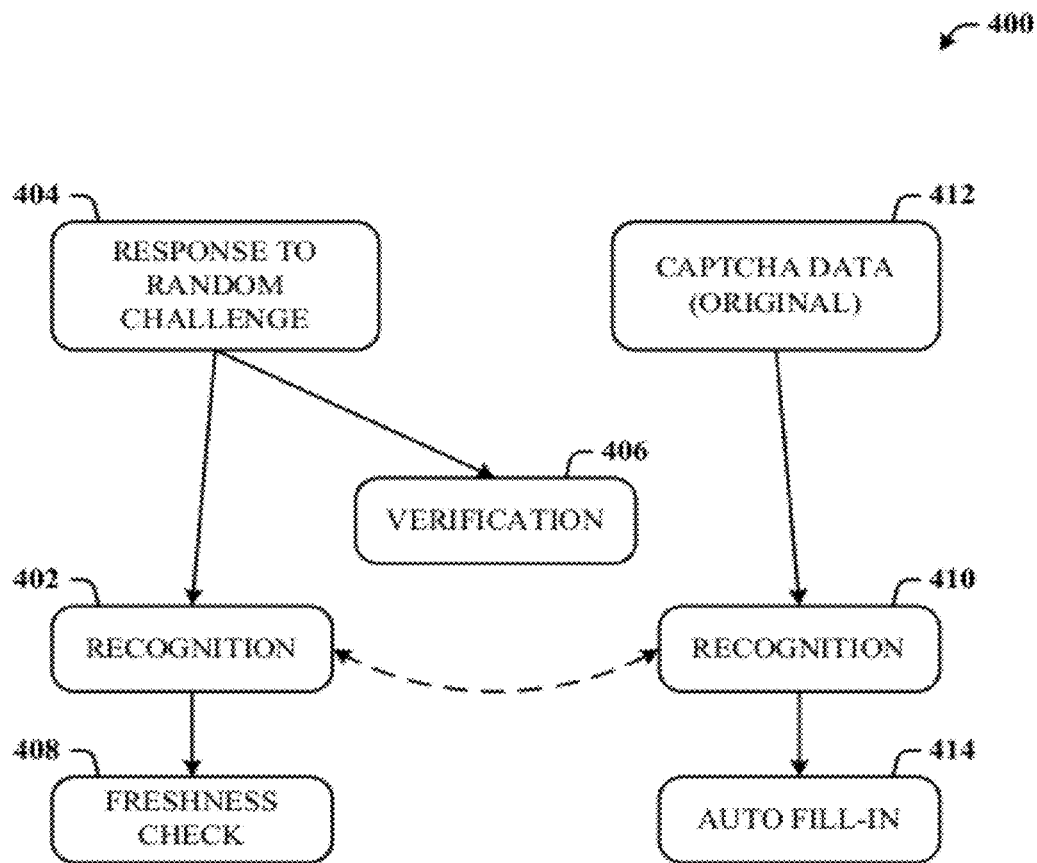


FIG. 3

**FIG. 4**

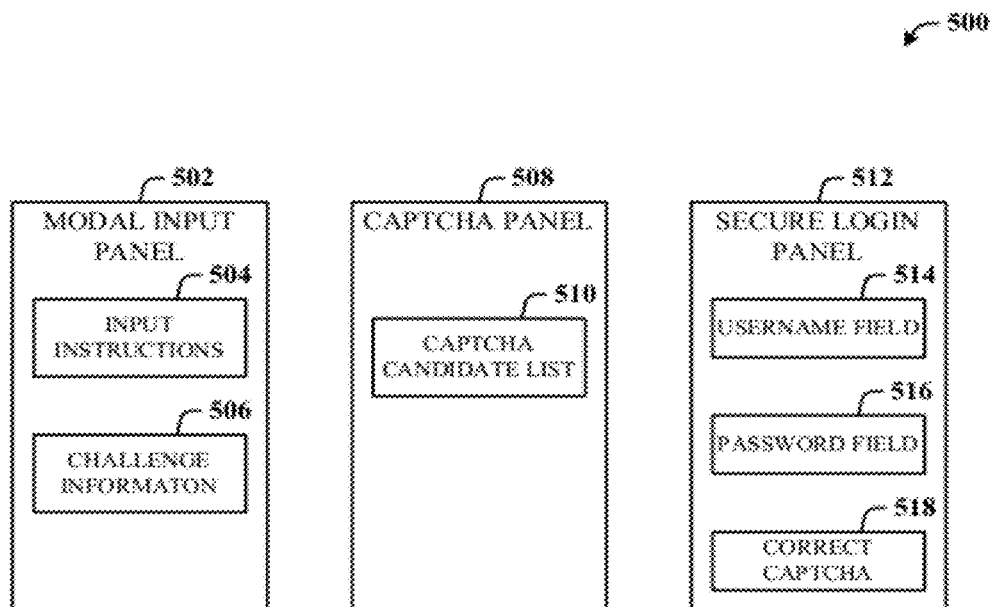
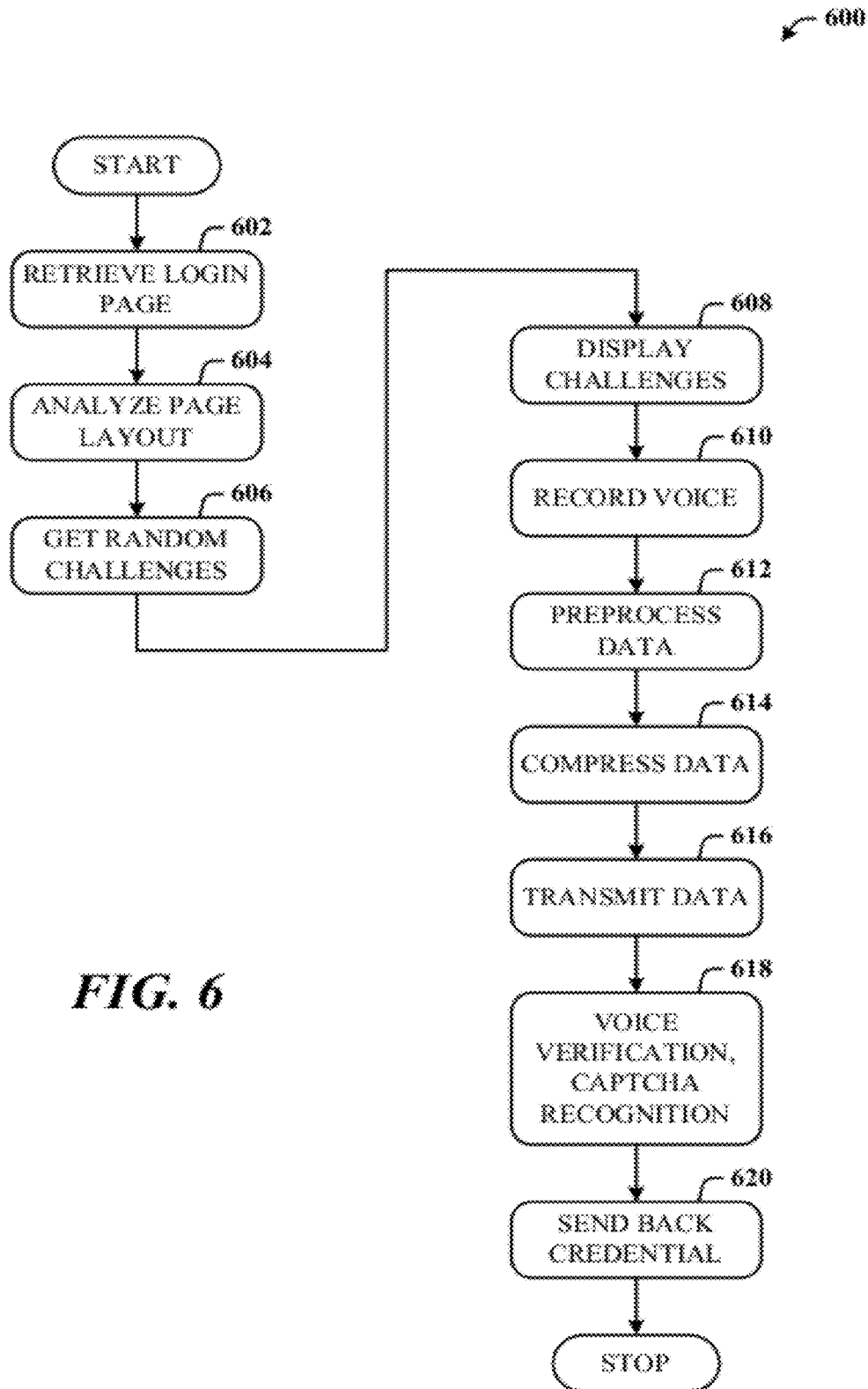
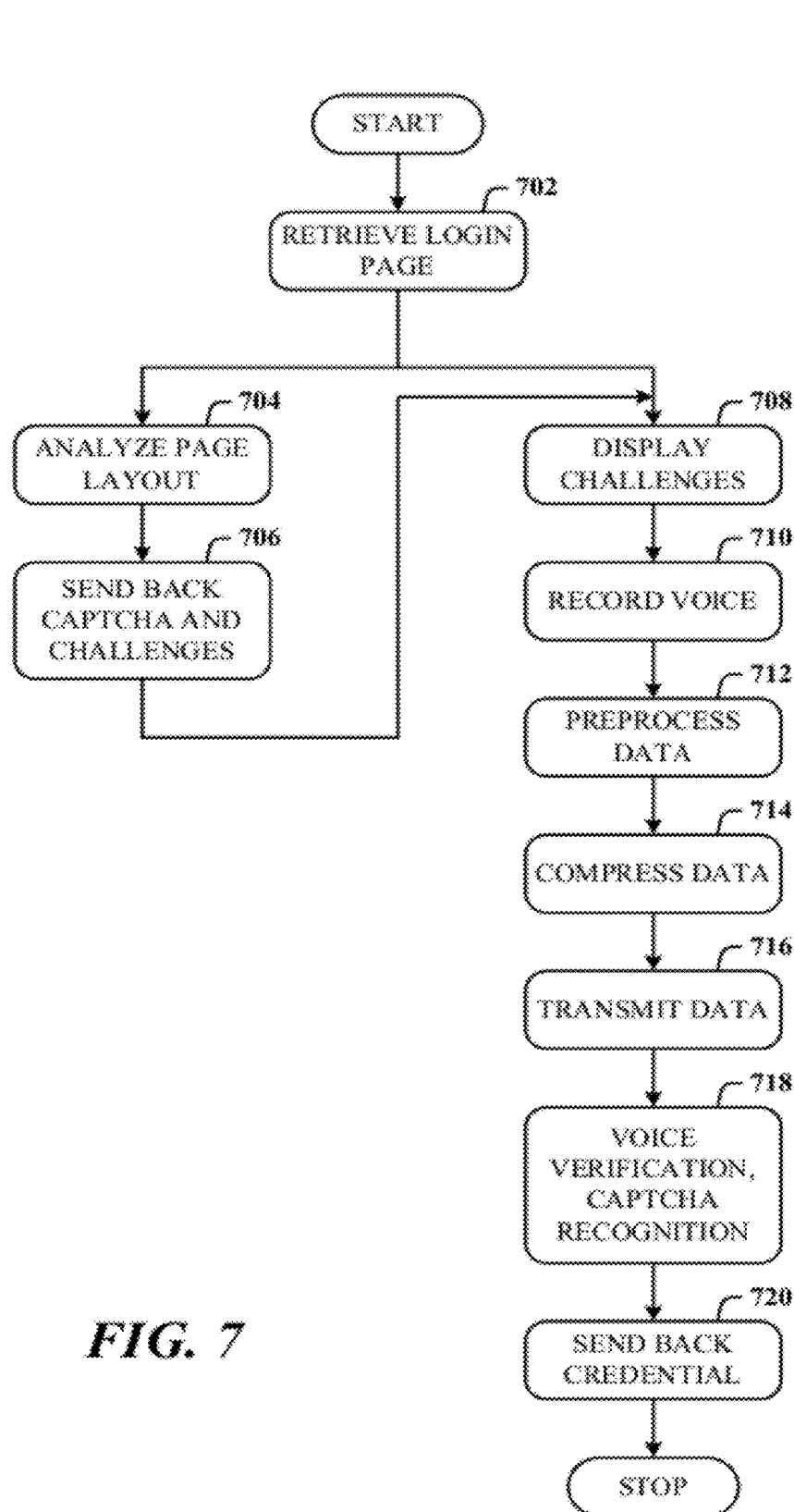
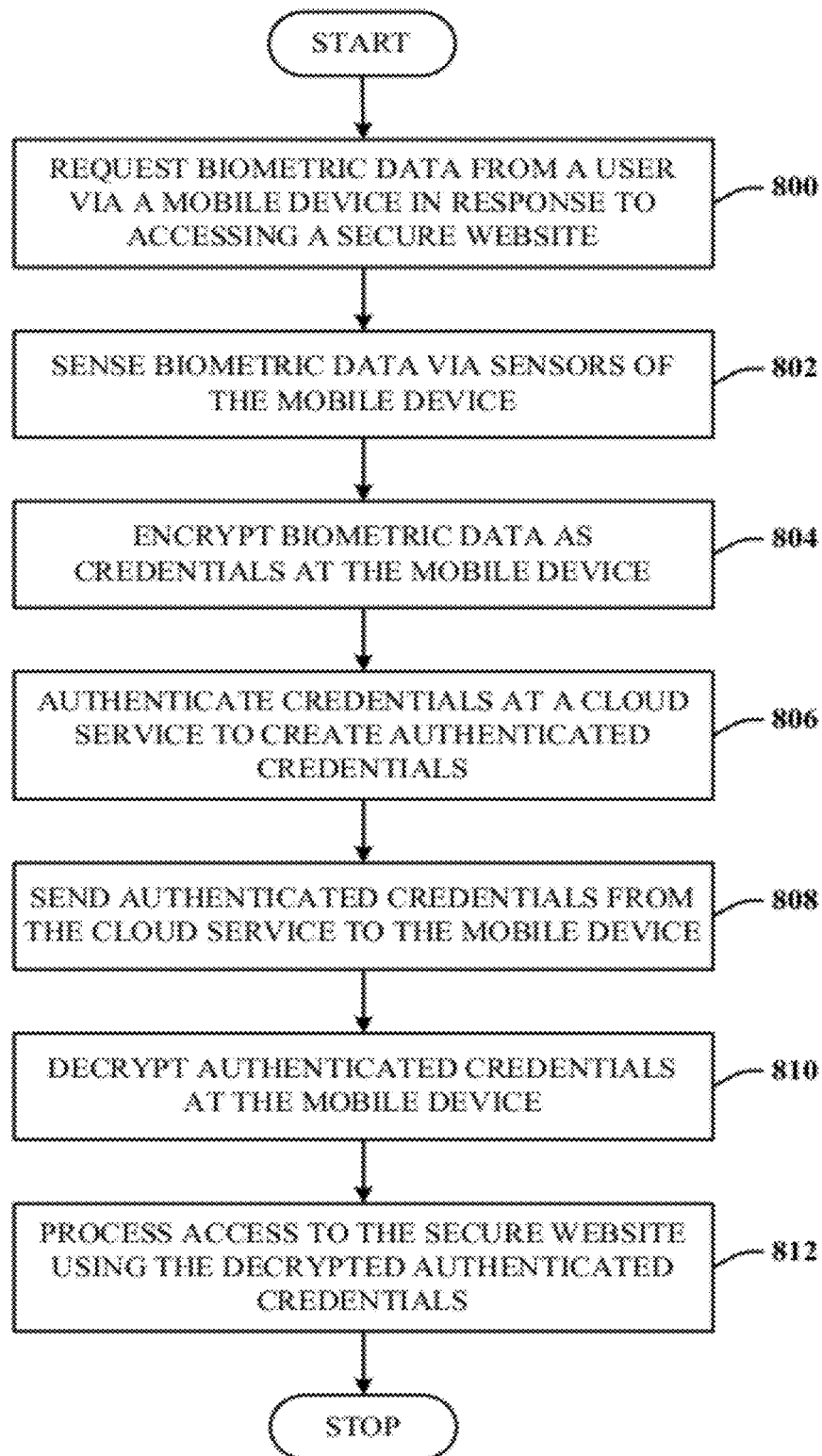
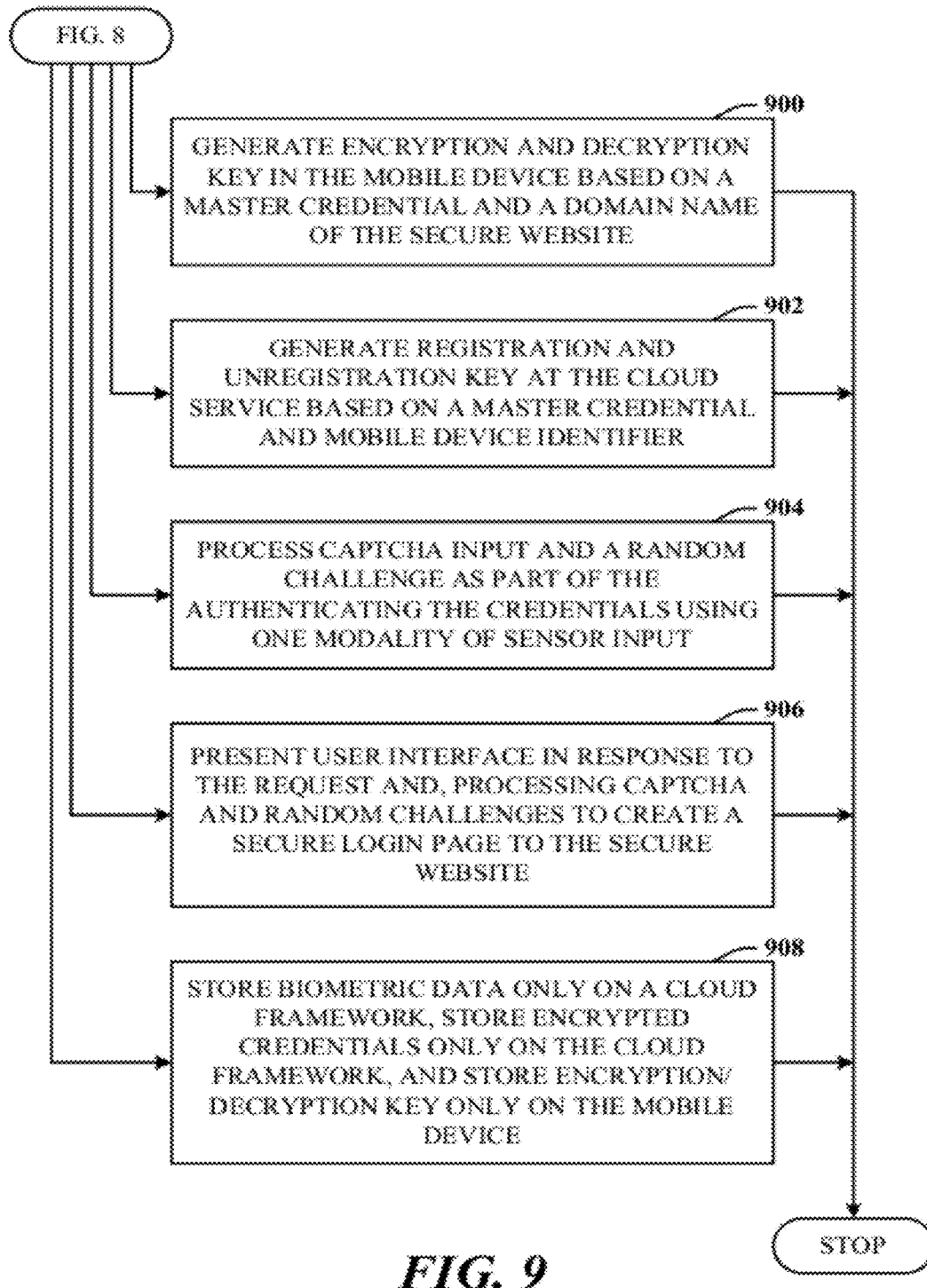


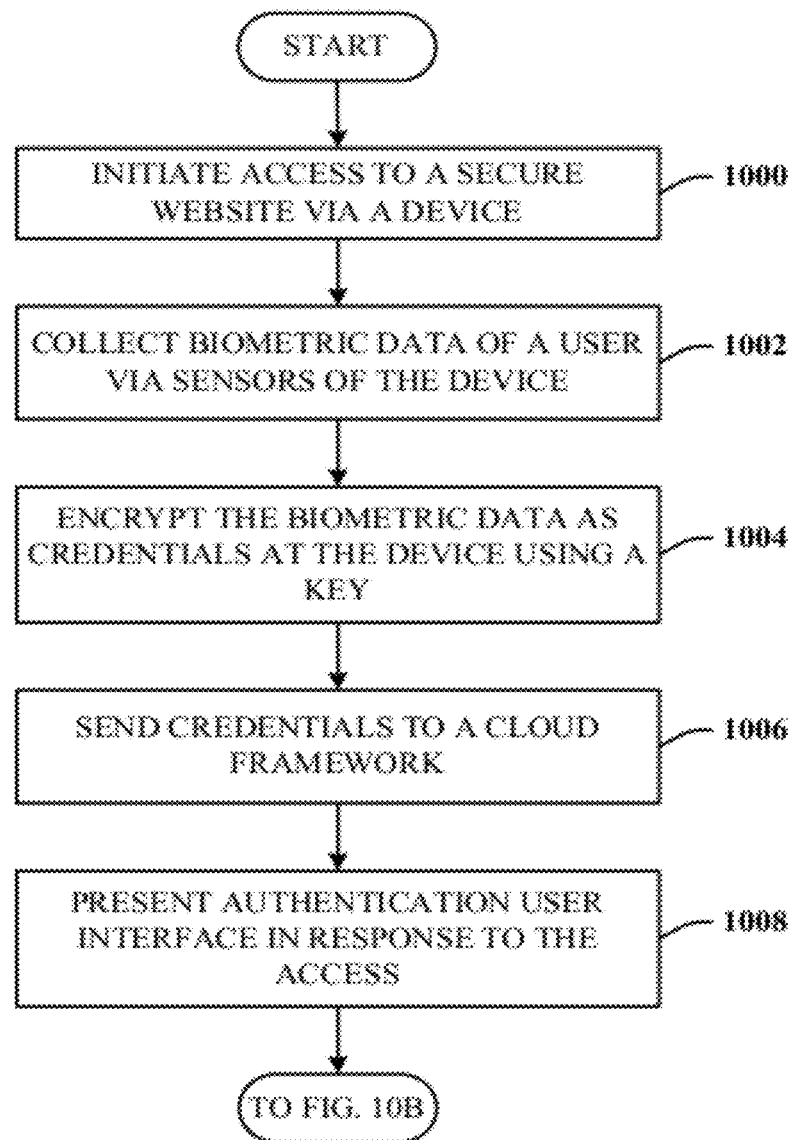
FIG. 5

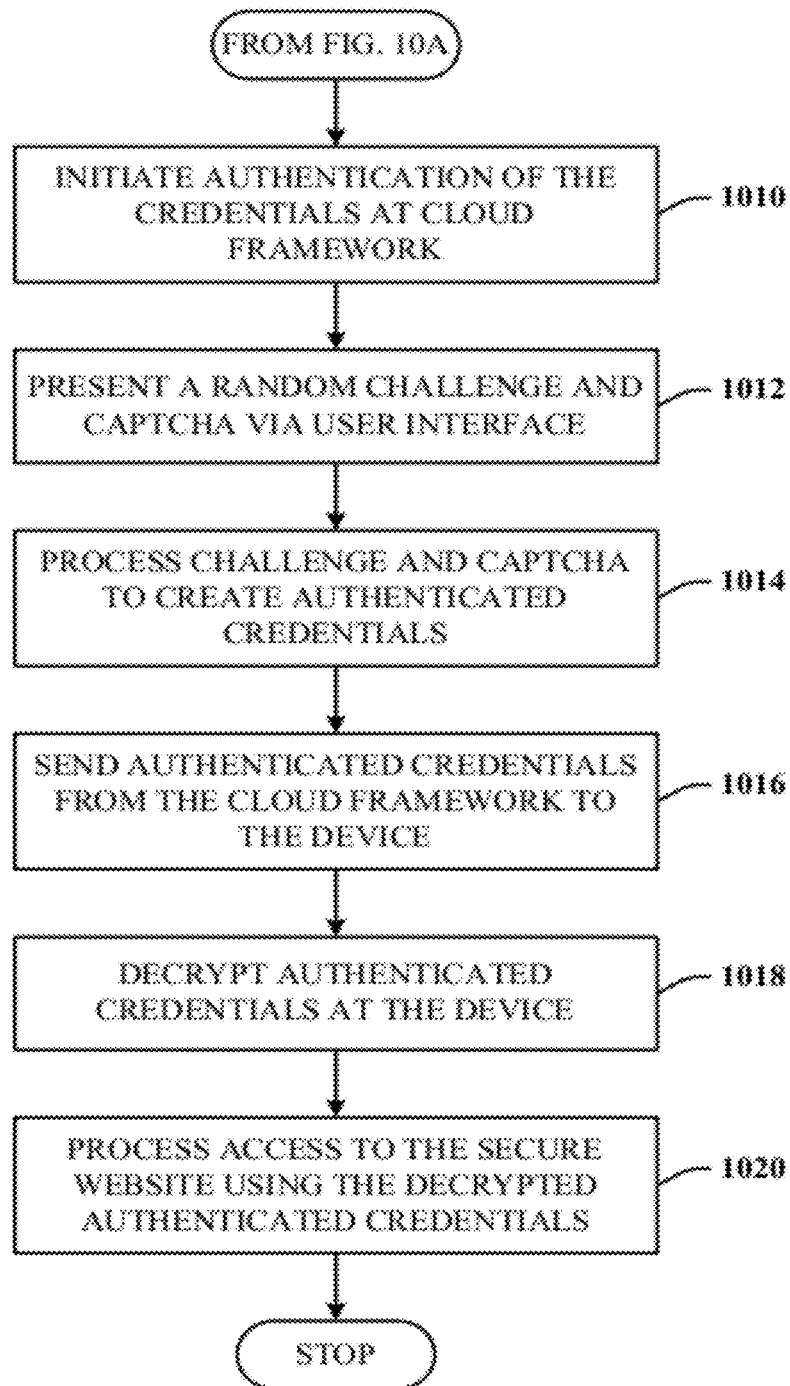


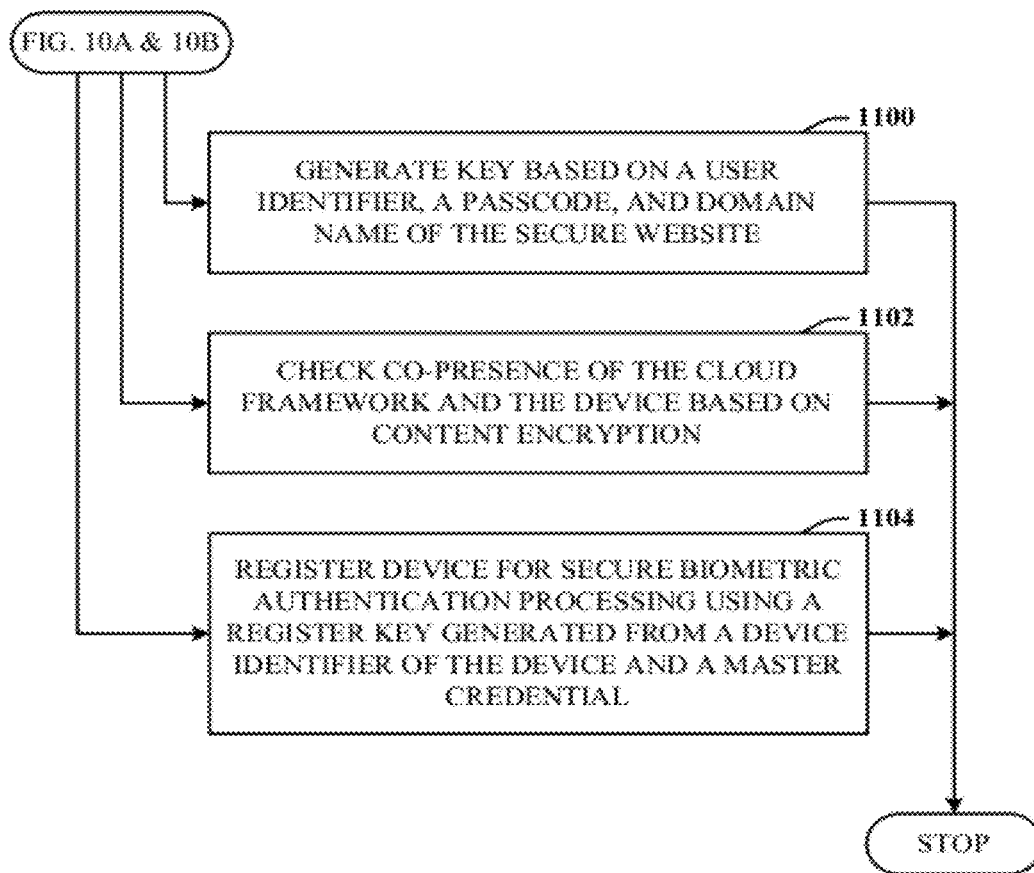


**FIG. 8**



**FIG. 10A**

**FIG. 10B**

**FIG. 11**

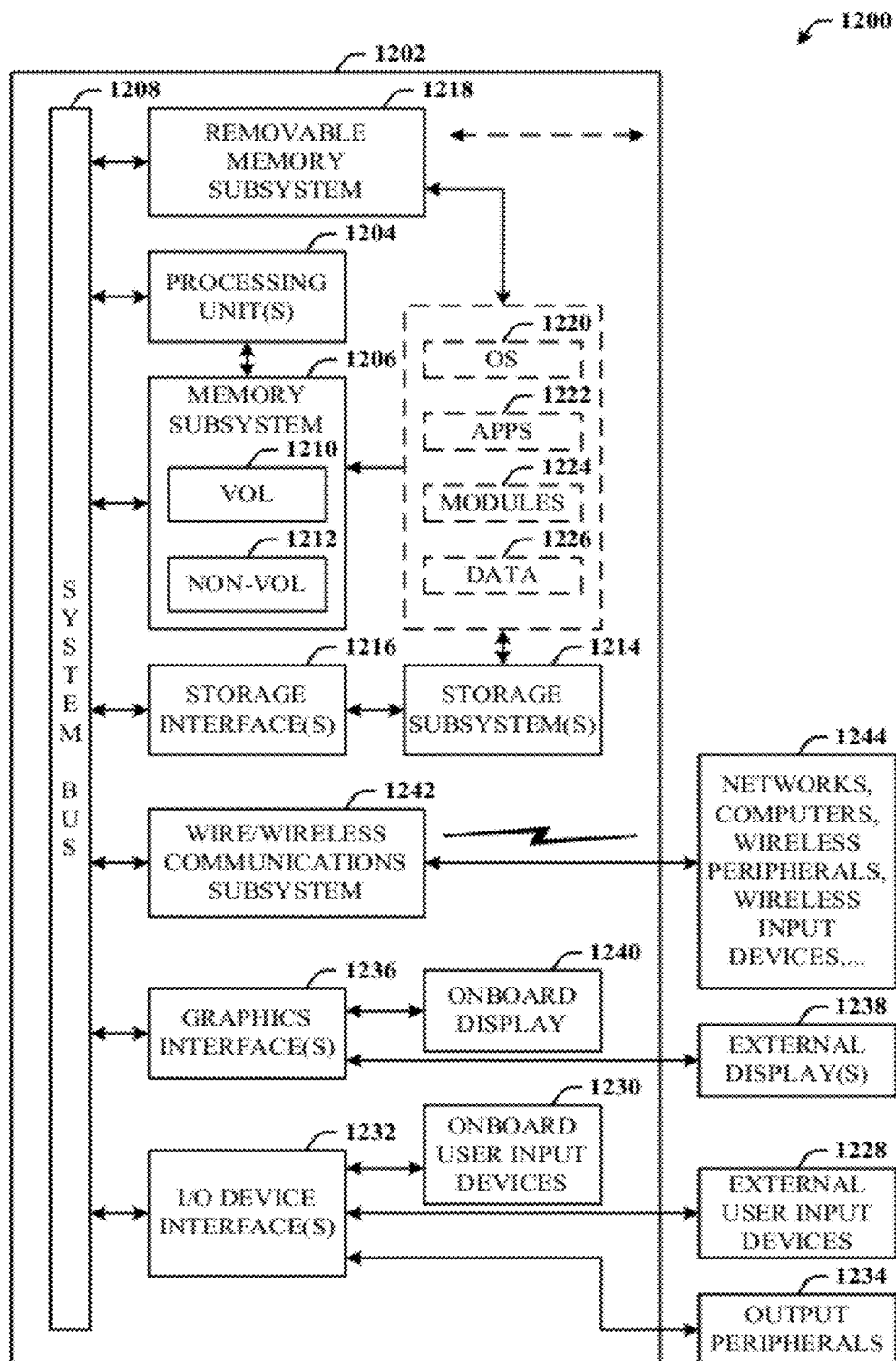


FIG. 12

1

USABLE SECURITY OF ONLINE PASSWORD MANAGEMENT WITH SENSOR-BASED AUTHENTICATION

BACKGROUND

The emergence of the mobile Internet, highly available cloud services, and mobile phones with rich on-phone sensing capabilities have significantly changed the landscape of mobile computing. Mobile Internet is gaining popularity with such magnitude that the number of users that connect to the Internet using mobile devices is expected to exceed that of desktop PCs within the few years.

Current security mechanisms that use passwords are appropriate for keyboard-equipped desktop PCs, but inconvenient for most mobile devices that typically have a much smaller form factor. As a best practice, secure websites unanimously enforce, or at least advise, the use of strong passwords that require both a minimum password length and diversity on the character set used (e.g., characters are a mix of upper and lower case letters, digits and non-alphanumeric characters). Stronger passwords improve security. However, it further increases the difficulty of inputting password on a mobile device, which usability drawbacks may eventually result in users counteracting practices, and hence, fail the original goal of security.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some novel embodiments described herein. This summary is not an extensive overview, and it is not intended to identify key/critical elements or to delineate the scope thereof. Its sole purpose is to present some concepts in a simplified form as a prelude to the more detailed description that is presented later.

The disclosed architecture is a multi-party security protocol that incorporates biometric based authentication and withstands attacks against any single party (e.g., mobile phone, cloud, or the user). The protocol involves the function split between mobile and cloud and the mechanisms to chain-hold the secrets. A key generation mechanisms binds secrets to a specific device or URL (uniform resource locator) by adding salt (e.g., random bits as one input to a one-way function) to a master credential. An inline CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) handling mechanism uses the same sensor modality as the authentication process, which not only improves the usability, but also facilitates the authentication process. A user friendly interface is also provided.

This architecture further enhances existing overall system security (e.g., handling untrusted or compromised cloud service, phone being lost, impersonation, etc.) and also improves the usability by automatically handling the CAPTCHA.

To the accomplishment of the foregoing and related ends, certain illustrative aspects are described herein in connection with the following description and the annexed drawings. These aspects are indicative of the various ways in which the principles disclosed herein can be practiced and all aspects and equivalents thereof are intended to be within the scope of the claimed subject matter. Other advantages and novel features will become apparent from the following detailed description when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates a security system in accordance with the disclosed architecture.

2

FIG. 2 illustrates security in a cloud framework in accordance with the disclosed architecture.

FIG. 3 illustrates an exemplary security software system for use on the client side.

FIG. 4 illustrates an exemplary inline CAPTCHA handling system.

FIG. 5 illustrates a user interface for random challenge and CAPTCHA input.

FIG. 6 illustrates a sequential work flow diagram of the security architecture for voice verification and recognition using a mobile device.

FIG. 7 illustrates an optimized sequential work flow diagram of the security architecture for voice verification and recognition using a mobile device that exploits parallelism.

FIG. 8 illustrates a security method in accordance with the disclosed architecture.

FIG. 9 illustrates further aspects of the method of FIG. 8.

FIG. 10A and FIG. 10B illustrate an alternative security method in accordance with the disclosed architecture.

FIG. 11 illustrates further aspects of the method of FIGS. 10A and 10B

FIG. 12 illustrates a block diagram of a computing system that executes a multi-party security protocol in accordance with the disclosed architecture.

DETAILED DESCRIPTION

Biometric information is now readily available from a number of different devices and in different forms. Thus, biometric-based authentication using sensors on cell phones, for example, provides a balance between security and usability. Mobile computing can be regarded as involving three separate parties: mobile phone, cloud, and user. Separation of these three lends itself to a three-party security protocol that incorporates biometric-based authentication and withstands attacks against any single party.

The disclosed architecture utilizes these three parties to enable user-friendly and secure mobile web access. Firstly, the use of biometric-based authentication strikes a balance between usability and security. This is particularly appropriate given the ever increasingly rich set of sensors that are now available, including on mobile devices. The proposed biometric authentication need not replace existing password-based authentication. Rather, the disclosed biometric authentication architecture can be used as an enhancement to the existing systems with improved usability and security.

Secondly, the architecture embraces the separation of mobile devices, users, and the cloud for security. A principal security challenge in mobile-cloud computing is that trust cannot be placed entirely on mobile devices (as such devices are susceptible to loss) or on the cloud (as the cloud may not be completely trustworthy). Rather, the architecture employs a security protocol that utilizes the physical separation of the three parties, where a user uses biometric authentication for self-identification, a cloud is used to store encrypted credentials, and the corresponding keys on mobile devices. In contrast to a conventional approach of using a cloud for computation offloading, the disclosed architecture uses a cloud for usability and security.

The architecture framework can accommodate different biometric authentication mechanisms, and is compatible with the current interactions between a client and a web service, in that eventually the same password-based credentials are supplied for authentication. This allows the architecture to be adopted without requiring any changes on web services.

Thirdly, for websites that use CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans

Apart) to distinguish real users from attacks from “robots”, the architecture allows users to handle CAPTCHA input by piggybacking on the user authentication process. Both authentication and recognition are performed on user actions, where authentication identifies a user using biometrics and recognition extracts the CAPTCHA input. For example, when using voice-based biometric authentication, the user is prompted to read the CAPTCHA and uses speech recognition to extract the input.

The disclosed architecture is an online password manager that utilizes biometric-authentication techniques (e.g., authentication through the biometric characteristics of human being such as face, voice, iris, vein, etc.), existing or otherwise, to maintain a mobile experience and at the same time increases the security level compared to traditional password managers.

The disclosed architecture reduces the risk of credential leakage as in traditional password managers by requiring users to pass the biometric-authentication before, at least, the automatic entry of user credentials (e.g., name, password, etc.). The devices that include a rich set of sensors, such as rich cell-phone sensors (e.g., camera and microphone) provide opportunities to utilize different biometric authentication techniques.

The disclosed architecture further relies on always-available cloud service(s) as a repository to maintain user credentials. There is no credential stored on the device (e.g., cell phone). Attackers cannot launch attacks to the storage system when having physical access to the phone. To address a concern of an untrusted cloud service, credentials are encrypted before deposited to the cloud repository. The key used to encrypt credentials, the encryption and decryption process, are all on the mobile device side. Therefore, the cloud is not able to eavesdrop the original credentials.

The disclosed architecture provides an improved user experience. The characteristics of human biometric are innate to users. The user does not need to remember anything to accommodate biometric authentication. For example, one way to input biometric information on a phone is simply to speak or take video clips. Thus, the burden in remembering and inputting the user name and password is reduced or eliminated entirely.

Additionally, name/password and CAPTCHA input is handled with one modality without sacrificing user experience. The same modality sensors are utilized to perform both authentication and CAPTCHA input.

Speech can be selected as a unified modality in one implementation. The system collects user voice to perform voice authentication and also performs speech recognition to handle CAPTCHA input. Other modalities such as face recognition are possible. Thus, a device can authenticate a user with face recognition and detect the CAPTCHA through the movement of the lips. An accelerometer and/or gyroscope can also be employed to capture user handwritings from which a user can be authenticated and CAPTCHA being recognized at the same time.

Reference is now made to the drawings, wherein like reference numerals are used to refer to like elements throughout. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding thereof. It may be evident, however, that the novel embodiments can be practiced without these specific details. In other instances, well known structures and devices are shown in block diagram form in order to facilitate a description thereof. The intention is to cover all modifications, equivalents, and alternatives falling within the spirit and scope of the claimed subject matter.

FIG. 1 illustrates a security system 100 in accordance with the disclosed architecture. As a general summary as to operation of the system 100 for a cell phone, for example, a user is prompted to input biometric data when attempting to access a secure website. The biometric data is captured by cell phone sensors. Authentication of the biometric data is then performed in the cloud. Authenticated encrypted credentials are returned from the cloud to the cell phone. The phone decrypts the credentials and uses a username and password to log-in to the secure website.

Upon encountering a secure web page that requires a user credential (e.g., a username and corresponding password), a cloud service is contacted. The service requests the user to input biometric data. The biometric data is captured by the corresponding on-premise (device and/or local external to the device) sensors and sent to the cloud side for authentication. If the user passes the bio-authentication, the corresponding encrypted credential is returned. The device then uses the on-phone key to decrypt it, automatically fill the derived user name and password into the corresponding fields of the web page, and submit to the original secure website.

During the process, the mobile user does not need to input any text-based password using the cumbersome on-phone keyboard. Instead, the user performs biometric-based authentication by video/audio recording, or other modal inputs.

The architecture employs separation of secrets. In other words, the credential is not stored on the user device (e.g., phone), but maintained on the cloud side. This reduces the risk of physical attack when the device is lost or stolen. The credential is encrypted when shipped to the cloud, so the cloud does not have the plain text, and the key for the credential encryption is not known to the cloud and employed on the mobile side. This reduces the concern on the untrusted cloud service. Moreover, the biometric information is held on the cloud side. The user device does not store the bio-information. Thus, attackers cannot obtain the biometric information by accessing the phone physically.

More specifically, the system 100 can include a security management component 102 (e.g., which includes a password manager) of a device 104 that processes a request 106 for access to a secure destination 108. In response to the access, the security management component 102 generates biometric data 110 of a user 112 of the device 104 in response to the request 106. The security management component 102 encrypts the biometric data 110 as encrypted credentials 114.

A cloud framework 116 performs authentication of the encrypted credentials 114 received from the device 104, and sends authenticated encrypted credentials 118 to the device 104. An encryption-decryption component 120 of the device 104 provides encryption-decryption processing such as for decrypting the authenticated encrypted credentials 118 to provide access information 122 to access the secure destination 108.

The biometric data 110 is stored (e.g., maintained during the time of registration) only on the cloud framework 116, the encrypted credentials 114 are stored (e.g., maintained during the time of registration) only on the cloud framework 116, and a decryption key for decrypting the authenticated encrypted credentials is stored (e.g., maintained during the time of registration) only on the device 104. The request 106 is received in response to access to a secure webpage of the secure destination 108, and the access information 122 includes a username and a password that are automatically input to access the secure destination 108. The encrypted credentials 114 are encrypted using a key created based on a master credential and domain information of the secure destination 108, and the key is correlated to the device 104.

5

The cloud framework **116** includes an inline CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) handling component **124** that concurrently presents a random challenge and the CAPTCHA to the user **112**, via the device **104** (which can be a mobile phone). The response to both the random challenge and the CAPTCHA is via a single sensor type (e.g., voice only, gesture only, etc.).

The cloud framework **116** includes a credential database that stores credentials, a model database of biometric models, and a layout database that stores parsed webpage login element information. The device **104** includes a browser plug-in that intercepts a login process to the secure destination **108**, analyzes webpage content to obtain a code input field, renders an authentication interface, and performs automatic form filling.

The system **100** can further comprise a sensor component **126** that includes local sensors which sense user biometrics related to at least one of face, voice, iris, or vein, and output sensor data as the biometric data **110**. The sensor component **126** performs recognition of a user interaction, and the security management component **102** prompts for further user input related to a type of the user interaction. In other words, if the user interaction is speech, the further user input prompted by the system **100** is also speech-based input.

The device **104** can optionally employ a security component (not shown) for opting in or out of exposing personal information by way of the sensor component **126**. The security component allows the subscriber to opt-in and opt-out of the capture of tracking information (e.g., geolocation) as well as personal information that may be obtainable. The user can be provided with notice of the collection of personal information, for example, and the opportunity to enable or deny consent to do so. Consent can take several forms. Opt-in consent imposes on the user to take an affirmative action before the data is collected. Alternatively, opt-out consent imposes on the user to take an affirmative action to prevent the collection of data before that data is collected.

The architecture ensures the co-presence of all the three legitimate parties (user, device, and cloud) before credentials can be retrieved. This is achieved by applying a physical separation principle. In a mobile device implementation, there are three parties involved in the overall work flow of the system, the user, the mobile device, and the cloud. The functionalities of a conventional password manager are now split between the mobile device and the cloud, and security is enhanced by the physical separation principle. Only from chain-holding of all the secrets can the system retrieve the website credentials.

The cloud side plays two roles. Firstly, the cloud serves as the central repository of user credentials. Secondly, the cloud performs biometric verification, and hence, also holds a repository of user biometric models. The mobile device also plays two roles accordingly. The device collects user biometrics via its sensors (and perhaps external sensors via short range wireless communications with the device), and performs pre-processing for performance optimization. The device can also perform automatic form filling when the credential is successfully retrieved from the cloud side.

The split between the user device and cloud has two manifests: the functionality of a conventional password manager, and the biometric authentication process. The split in the manager offers a possibility to handle an untrusted cloud and mitigates the possible information leakage when the device gets lost or the cloud is compromised. The split in the biometric authentication allows the incorporation of complex

6

algorithms in the device-cloud computing for higher biometric detection accuracy, using the rich in-cloud computing resources.

With the device-cloud split, the co-presence of the device and cloud is enforced by content encryption. Credentials stored on the cloud side are encrypted while the encryption/decryption key is held by the device. Biometric authentication is performed to ensure the presence of the correct user. Only when the user passes the biometric authentication will the cloud return encrypted credentials.

FIG. 2 illustrates security in a cloud framework **200** in accordance with the disclosed architecture. The cloud framework **200** includes three data repositories (also referred to as databases): a credentials database **202** that stores credentials, a model database **204** that stores user biometric data, and a CAPTCHA layout database **206** that stores the page layout of the secure website, as obtained from a page layout analyzer **208**. The cloud framework **200** can also include three function modules: a freshness check module **210** that checks freshness of the biometric input, an authentication module **212** that performs biometric authentication, and a CAPTCHA recognition module **214** that conducts page layout analysis. The CAPTCHA recognition module **214** A server **216** provides a set of web service APIs (WS API) to the device for bio-authentication. The authentication module **212** provides input to a model update module **218**, to further update the model database **204** of model stored therein. An output of the authentication module **212** is an authentication result **220**, which is passed to the device. The device includes the sensor component **126** (of FIG. 1), which provides sensor data or device features **222** to the freshness check module **210** for freshness checks.

In other words, the credential repository is a collection of URL indexed credential records. Each record can be in the format of $[f(url), f(DevID), K_{enc}(credential)]$, where K_{enc} is an encryption key, described in detail hereinbelow. The biometric model repository stores various biometric models, together with the associated feature parameters and the decision thresholds for the specific bio-authentication means.

The freshness check module **210** scrutinizes the freshness of the user's biometric data. If there is CAPTCHA on the login page, the freshness check module **210** generates random challenges suitable for the chosen sensor modality. Upon receiving responses from the device, the freshness check module **210** recognizes the random challenge and compares it against a ground truth. The biometric authentication module **212** will only perform the user verification if the freshness check passes.

The page layout analyzer **208** parses the login pages of all the secure websites the user has registered, and extracts the HTML (hypertext markup language) elements of the input field name or identifier (ID) for username, password, and CAPTCHA, and the position of these fields in a DOM (document object model) tree. Such information is stored in the layout repository.

The device communicates to the cloud through the WS APIs. The communication can be protected using SSL (secure socket layer). Additionally, the Hash(DevID) is mandatory parameter in all of the WS APIs, which discourages a random scanning attack. Absent this parameter, an attacker might be able to easily hit victim systems through scanning using randomly grabbed biometric signals, due to relatively low entropy of biometric signals.

FIG. 3 illustrates an exemplary security software system **300** for use on the client side. The client-side software enables direct access of hardware sensors from within a browser (e.g., mobile). (Another solution may include the use of HTML5 in

the client device browser.) In this implementation, a combination of a browser plug-in **302** of a device browser **304** and a local web server **306** is employed. The browser plug-in **302** can access the raw content of a secure webpage (since the content is already decrypted). The plug-in **302** intercepts the login process, analyzes the page content to obtain the CAPTCHA input field, renders the authentication user interface, and performs automatic form filling. The local server **306** accesses local hardware sensors **308**, communicates with the cloud framework **116** (also called service), and performs encryption/decryption. The local server **306** can also perform certain pre-processing and/or feature extraction to speed-up the whole process.

Accordingly, the local server **306** can include a CAPTCHA layout cache **310**, a pre-processing module **312**, and an encryption/decryption module **314**. The sensors **308** can include many common sensors typically employed with the user device such as a camera **316** (video or still), microphone **318**, motion sensor **320** (e.g., accelerometer, tilt, etc.), and location sensor **322** (e.g., geolocation subsystem such as GPS (global positioning system)).

In an alternative implementation that is not browser-specific, similar results can be achieved by deploying an SSL proxy to hijack the original HTTPS (hypertext transfer protocol secure) session and split the session into two HTTPS sessions.

FIG. 4 illustrates an exemplary inline CAPTCHA handling system **400**. The CAPTCHA system is inline in that the CAPTCHA input is handled within the process of biometric authentication (bio-authentication) using one modality of sensor input, without interruption. During the bio-authentication, one or more random challenges and the CAPTCHA are displayed to the user concurrently. The user inputs the challenges and CAPTCHA using one type of sensor (e.g., microphone, accelerometer). For example, if the user employs gesture as the authentication method, the system **400** can attempt recognition of the CAPTCHA via handwriting recognition.

The inline CAPTCHA handling system **400** improves the user experience. Additionally, since the ground truth of the response is known to the cloud, the random challenge can serve to train biometric data, which the cloud can accumulatively utilize to incrementally improve the recognition accuracy for the CAPTCHA input.

The inline CAPTCHA handling system **400** is described in a voice authentication example. The user reads both the random challenge sent from the cloud service and the CAPTCHA sent from the website of interest. Using voice input, the cloud side performs the following tasks: recognition **402** of the random words via speech recognition, as provided as a response **404** to a random challenge, and performs verification **406** of the correctness of the voice response **404**. If the sensor data is correct, a freshness check **408** is passed. If voice verification **406** is successful, then CAPTCHA recognition **410** is performed on CAPTCHA data **412**. The user's voice for random words may be used as on-the-fly training data. The credential and CAPTCHA recognition result are both returned to the client for processing and auto fill-in **414**.

FIG. 5 illustrates a user interface **500** for random challenge and CAPTCHA input. The user interface **500** is described in terms of voice recognition and authentication as the modal input. A modal input panel **502** can be a popup window that prompts for user input. In this example, the modal input panel **502** can present input instructions **504** as to what modal input

is to be used and challenge information **506** as to the user response (e.g., spoken letters, characters, words, etc.) to the challenge.

A CAPTCHA panel **508** can be a pop-up window that presents CAPTCHA output as multiple possible recognition results for viewing by the user at the client device. Presentation can be ranked candidate list **510** with the most likely candidate at the top. The user selects the correct candidate from the list **510**, and continues the login process. If no selection in the list **510** is correct, the user will need to perform a correction such as repeating the process to make the correct selection. Finally, the credential and CAPTCHA are automatically filled-in on the target webpage, as shown in a secure login panel **512** of the web service. The credentials can include auto-entry of a username in a username field **514**, auto-entry of a password in a password field **516**, and presentation of the correct CAPTCHA **518**.

Following is a description of secrets chain-holding and key generation for both encryption/decryption and registration.

The disclosed architecture includes biometric data (K_{bio}) of the real user, a key (K_{enc}) for encryption/decryption of credentials (assumes the use of symmetric key cryptography), and a device token (Token). The three parties in play include the device user, the device, and the cloud. According to a threat model, any party can be untrusted (e.g., the device user can be an impostor).

According to the physical separation principle, K_{bio} is held by the cloud, K_{enc} is held by the device, and Token is held by a user. Only when the correct K_{bio} , K_{enc} , and the Token are all present, can the architecture retrieve the plaintext of the credentials.

With respect to key generation, when a user registers with the disclose security architecture, the user chooses a master credential (MC) (the master credential is secured and used for input when registering, unregistering, and in rescue mode) that comprises an ID (e.g., a unique ID such as an email address) and a strong passcode. The MC and the domain name of the targeted website (URL) are used as a seed to generate K_{enc} :

$$K_{enc} = f(\text{concat}(\text{URL}, \text{MC}))$$

where $\text{concat}()$ is to concatenate two strings, and $f()$ is a secure cryptographic hash function (e.g., SHA-1). The key K_{enc} is then used for credential encryption and decryption.

To register and unregister a device such as a mobile phone, the architecture uses the master credential (MC) to generate a registration key, K_{reg} , which is defined as,

$$K_{reg} = f(\text{xor}(\text{MC}, \text{DevID}))$$

where DevID is a unique device ID (e.g., IMEI (international mobile equipment identity) number). The registration key K_{reg} is stored only on the cloud side. The registration key is sent to security service of the cloud framework at device registration time. The cloud service uses K_{reg} to unregister a device from the security service. The registration key K_{reg} is also a rescue means for the user to authenticate the user by conventional password authentication, when the user fails the biometric authentication. In this rescue mode, the device uses a different encryption strategy: the device first derives the plaintext of K_{reg} from MC (which is input by the user). The device further encrypts the plaintext using K_{reg} (instead of K_{enc} so that the server can decrypt it) and sends the encrypted credentials to the server. The server compares the decrypted content against its own copy.

Note that, salt (DevID and URL) has been added when generating K_{reg} and K_{enc} . DevID correlates K_{reg} not only to

MC, but also the mobile device. Thus, this discourages random guess on the MC across multiple security users.

Incorporating website's URL in generating K_{enc} avoids a "crack one for all" effect, since now, each secure site has a different encryption key. Incorporating the URL also reduces the risk when users reuse the password extensively across multiple websites.

Following is a general description of a threat model. The physical separation of the encryption key (K_{enc}), biometric data (K_{bio}), and the device token (Token) to different parties ensures that the absence of any party in the chain will fail the retrieval of the original credential.

For the threat of the client device being lost/stolen, since no password is stored on the device, there is no worry about the credential leak. The malicious phone holder does not possess K_{bio} , hence the holder cannot retrieve the credential from the cloud. If the holder launches a random attack to the cloud using the device, the cloud can lock the device for a certain number of retries.

For the untrusted cloud threat, as the credential is encrypted, the attacker cannot retrieve the plaintext. Moreover, the addition of salt to generate keys makes it more difficult to for the system to be cracked.

With respect to spoofing the biometric data, the freshness process of the K_{bio} provides a means for defeating this attack. The architecture can adopt the standard challenge-response method to ensure the fresh capture of biometric data. The user finishes the biometric data input within a predefined period of time. Hence, simply forging and replaying stale biometric data cannot break the system. Moreover, even if the attacker successfully spoofs the bio-authentication mechanism, it is similar to that of the untrusted cloud case, which does not immediately result in information leakage thanks to the separation of secrets. Thus, the disclosed architecture demonstrates improved security over conventional biometric authentication systems.

Additionally, a key revocation mechanism is provided that allows use of the master credential MC to configure the cloud service to stop further access from the lost device to protect user credentials when both the device is stolen and the biometric signal is also spoofed by the same attacker.

FIG. 6 illustrates a sequential work flow diagram 600 of the security architecture for voice verification and recognition using a mobile device. Initially, the security architecture renders the received CAPTCHA (from the targeted secure website) and the random challenge from cloud service, in one page (FIG. 5). The rendering action depends on the CAPTCHA, the challenge word, and the CAPTCHA layout information stored in the cloud. The system parallelizes the requests from the mobile device to the targeted website and the cloud service. The retrieval of CAPTCHA, analysis of layout of the login webpage, and the generation of random challenge can be executed in parallel.

According to the diagram 600, the mobile device retrieves a login page based on access request of the secure website, as indicated at 602. Upon receiving the request from the mobile device, the cloud page layout analyzer (208 of FIG. 2) emulates a mobile request to the targeted secure website, analyzes the layout of returned pages to identify the HTML element of the CAPTCHA fields and the node positions of these fields in the DOM tree, as indicated at 604. The information is saved to the page layout repository (layout database 206) and also sent back to the mobile device, along with the random challenges of suitable length. Since websites rarely change the login page layout, for consistent user experience, page layout analysis is lazily performed, on a daily basis, for example. The page layout repository (layout database 206) saves an

on-demand request to the specific requested secure website. Note that, the page layout information is user independent, and hence, can be shared among all architecture users.

At 606, random challenges are obtained. At 608, the random challenges are presented. At 610, the user voice is recorded as biometric data. At 612, the voice biometric data is pre-processed (e.g., silence detection and removal, and self normalization). At 614, the biometric data is compressed for transmission. At 616, the compressed data is transmitted. At 618, voice verification and CAPTCHA recognition is performed. At 620, an authenticated credential is sent back to the mobile device.

FIG. 7 illustrates an optimized sequential work flow diagram 700 of the security architecture for voice verification and recognition using a mobile device that exploits parallelism. The diagram exploits parallelism among subtasks and also shifts certain tasks to the cloud. The averaged effect of parallelizing requests over WiFi (wireless fidelity), 3G (3rd generation mobile telecommunications), and GPRS (general packet radio service) network provides enhanced performance.

Pipelining is another way to exploit parallelism. The audio signal is usually processed on a frame-by-frame basis and has no temporal dependency. The processing stages can be pipelined. The pre-processing 312 involves at least two function modules: silence detection and removal using a zero-crossing algorithm, and self normalization that adapts the voice signal to the noise floor. Additionally, a standard AMR (adaptive multi-rate) codec (coder/decoder) can be utilized to compress the resulting voice segments before transmission.

In this flow diagram 700, parallelism involves retrieving the login page. In one leg of the diagram 700, the login page is retrieved, at 702. At 704, the layout of the page is analyzed. At 706, CAPTCHA and challenges are sent back. While this processing occurs, the login page retrieval, at 702, also occurs to prepare for display of challenges, at 708. At 710, the user voice is recorded as biometric data. At 712, the voice biometric data is pre-processed (e.g., silence detection and removal, and self normalization). At 714, the biometric data is compressed for transmission. At 716, the compressed data is transmitted. At 718, voice verification and CAPTCHA recognition is performed. At 720, an authenticated credential is sent back to the mobile device.

FIG. 6 and FIG. 7 describe flow for application of the disclosed architecture to voice verification and recognition. However, it is to be understood that this is only one application, and can be generalized to other modalities. For example, block 610 can capture sensor data, and thus, block 618 is then biometric verification and CAPTCHA recognition. This applies similarly to blocks 710 and 718 of FIG. 7.

Included herein is a set of flow charts representative of exemplary methodologies for performing novel aspects of the disclosed architecture. While, for purposes of simplicity of explanation, the one or more methodologies shown herein, for example, in the form of a flow chart or flow diagram, are shown and described as a series of acts, it is to be understood and appreciated that the methodologies are not limited by the order of acts, as some acts may, in accordance therewith, occur in a different order and/or concurrently with other acts from that shown and described herein. For example, those skilled in the art will understand and appreciate that a methodology could alternatively be represented as a series of inter-related states or events, such as in a state diagram. Moreover, not all acts illustrated in a methodology may be required for a novel implementation.

FIG. 8 illustrates a security method in accordance with the disclosed architecture. At 800, biometric data of a user is

11

requested via a mobile device in response to accessing a secure website. At **802**, the biometric data is sensed via sensors of the mobile device. At **804**, the biometric data is encrypted as credentials at the mobile device. At **806**, the credentials are authenticated at a cloud service to create authenticated credentials. At **808**, the authenticated credentials are sent from the cloud service to the mobile device. At **810**, the authenticated credentials are decrypted at the mobile device. At **812**, access to the secure website is processed using the decrypted authenticated credentials.

FIG. **9** illustrates further aspects of the method of FIG. **8**. Note that the flow indicates that each block can represent a step that can be included, separately or in combination with other blocks, as additional aspects of the method represented by the flow chart of FIG. **8**. At **900**, an encryption and decryption key is generated in the mobile device based on a master credential and a domain name of the secure website. At **902**, a registration and unregistration key is generated at the cloud service based on a master credential and mobile device identifier. At **904**, a CAPTCHA input and a random challenge are processed as part of the authenticating the credentials using one modality of sensor input. At **906**, a user interface is presented in response to the request and, processing CAPTCHA and random challenges to create a secure login page to the secure website. At **908**, the biometric data is stored only on a cloud framework, the encrypted credentials are stored only on the cloud framework, and an encryption/decryption key is stored only on the mobile device.

FIG. **10A** and FIG. **10B** illustrate an alternative security method in accordance with the disclosed architecture. At **1000**, access to a secure website is initiated via a device. At **1002**, biometric data of a user is collected via sensors of the device. At **1004**, the biometric data is encrypted as credentials at the device using a key. At **1006**, the credentials are sent to a cloud framework. At **1008**, an authentication user interface is presented in response to the access. Continuing to FIG. **10B**, at **1010**, authentication of the credentials is initiated at the cloud framework. At **1012**, a random challenge and CAPTCHA are presented via the user interface. At **1014**, the challenge and CAPTCHA are processed to create authenticated credentials. At **1016**, the authenticated credentials are sent from the cloud framework to the device. At **1018**, the authenticated credentials are decrypted at the device. At **1020**, access to the secure website is processed using the decrypted authenticated credentials.

FIG. **11** illustrates further aspects of the method of FIGS. **10A** and **10B**. Note that the flow indicates that each block can represent a step that can be included, separately or in combination with other blocks, as additional aspects of the method represented by the flow chart of FIG. **10**. At **1100**, the key is generated based on a user identifier, a passcode, and domain name of the secure website. At **1102**, co-presence of the cloud framework and the device is checked based on content encryption. At **1104**, the device is registered for secure biometric authentication processing using a register key generated from a device identifier of the device and a master credential.

As used in this application, the terms “component” and “system” are intended to refer to a computer-related entity, either hardware, a combination of software and tangible hardware, software, or software in execution. For example, a component can be, but is not limited to, tangible components such as a processor, chip memory, mass storage devices (e.g., optical drives, solid state drives, and/or magnetic storage media drives), and computers, and software components such as a process running on a processor, an object, an executable, a data structure (stored in volatile or non-volatile storage

12

media), a module, a thread of execution, and/or a program. By way of illustration, both an application running on a server and the server can be a component. One or more components can reside within a process and/or thread of execution, and a component can be localized on one computer and/or distributed between two or more computers. The word “exemplary” may be used herein to mean serving as an example, instance, or illustration. Any aspect or design described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other aspects or designs.

Referring now to FIG. **12**, there is illustrated a block diagram of a computing system **1200** that executes a multi-party security protocol in accordance with the disclosed architecture. However, it is appreciated that the some or all aspects of the disclosed methods and/or systems can be implemented as a system-on-a-chip, where analog, digital, mixed signals, and other functions are fabricated on a single chip substrate. In order to provide additional context for various aspects thereof, FIG. **12** and the following description are intended to provide a brief, general description of the suitable computing system **1200** in which the various aspects can be implemented. While the description above is in the general context of computer-executable instructions that can run on one or more computers, those skilled in the art will recognize that a novel embodiment also can be implemented in combination with other program modules and/or as a combination of hardware and software.

The computing system **1200** for implementing various aspects includes the computer **1202** having processing unit(s) **1204**, a computer-readable storage such as a system memory **1206**, and a system bus **1208**. The processing unit(s) **1204** can be any of various commercially available processors such as single-processor, multi-processor, single-core units and multi-core units. Moreover, those skilled in the art will appreciate that the novel methods can be practiced with other computer system configurations, including minicomputers, mainframe computers, as well as personal computers (e.g., desktop, laptop, etc.), hand-held computing devices, micro-processor-based or programmable consumer electronics, and the like, each of which can be operatively coupled to one or more associated devices.

The system memory **1206** can include computer-readable storage (physical storage media) such as a volatile (VOL) memory **1210** (e.g., random access memory (RAM)) and non-volatile memory (NON-VOL) **1212** (e.g., ROM, EPROM, EEPROM, etc.). A basic input/output system (BIOS) can be stored in the non-volatile memory **1212**, and includes the basic routines that facilitate the communication of data and signals between components within the computer **1202**, such as during startup. The volatile memory **1210** can also include a high-speed RAM such as static RAM for caching data.

The system bus **1208** provides an interface for system components including, but not limited to, the system memory **1206** to the processing unit(s) **1204**. The system bus **1208** can be any of several types of bus structure that can further interconnect to a memory bus (with or without a memory controller), and a peripheral bus (e.g., PCI, PCIe, AGP, LPC, etc.), using any of a variety of commercially available bus architectures.

The computer **1202** further includes machine readable storage subsystem(s) **1214** and storage interface(s) **1216** for interfacing the storage subsystem(s) **1214** to the system bus **1208** and other desired computer components. The storage subsystem(s) **1214** (physical storage media) can include one or more of a hard disk drive (HDD), a magnetic floppy disk drive (FDD), and/or optical disk storage drive (e.g., a CD-

13

ROM drive DVD drive), for example. The storage interface(s) **1216** can include interface technologies such as EIDE, ATA, SATA, and IEEE 1394, for example.

One or more programs and data can be stored in the memory subsystem **1206**, a machine readable and removable memory subsystem **1218** (e.g., flash drive form factor technology), and/or the storage subsystem(s) **1214** (e.g., optical, magnetic, solid state), including an operating system **1220**, one or more application programs **1222**, other program modules **1224**, and program data **1226**.

The operating system **1220**, one or more application programs **1222**, other program modules **1224**, and/or program data **1226** can include the entities and components of the system **100** of FIG. 1, the entities and components of the framework **200** of FIG. 2, the entities and components of the system **300** of FIG. 3, the entities and components of the system **400** of FIG. 4, the user interface **500** of FIG. 5, the flow diagrams **600** and **700** of FIGS. 6 and 7, and the methods represented by the flowcharts of FIGS. 8-11, for example.

Generally, programs include routines, methods, data structures, other software components, etc., that perform particular tasks or implement particular abstract data types. All or portions of the operating system **1220**, applications **1222**, modules **1224**, and/or data **1226** can also be cached in memory such as the volatile memory **1210**, for example. It is to be appreciated that the disclosed architecture can be implemented with various commercially available operating systems or combinations of operating systems (e.g., as virtual machines).

The storage subsystem(s) **1214** and memory subsystems (**1206** and **1218**) serve as computer readable media for volatile and non-volatile storage of data, data structures, computer-executable instructions, and so forth. Such instructions, when executed by a computer or other machine, can cause the computer or other machine to perform one or more acts of a method. The instructions to perform the acts can be stored on one medium, or could be stored across multiple media, so that the instructions appear collectively on the one or more computer-readable storage media, regardless of whether all of the instructions are on the same media.

Computer readable media can be any available media that can be accessed by the computer **1202** and includes volatile and non-volatile internal and/or external media that is removable or non-removable. For the computer **1202**, the media accommodate the storage of data in any suitable digital format. It should be appreciated by those skilled in the art that other types of computer readable media can be employed such as zip drives, magnetic tape, flash memory cards, flash drives, cartridges, and the like, for storing computer executable instructions for performing the novel methods of the disclosed architecture.

A user can interact with the computer **1202**, programs, and data using external user input devices **1228** such as a keyboard and a mouse. Other external user input devices **1228** can include a microphone, an IR (infrared) remote control, a joystick, a game pad, camera recognition systems, a stylus pen, touch screen, gesture systems (e.g., eye movement, head movement, etc.), and/or the like. The user can interact with the computer **1202**, programs, and data using onboard user input devices **1230** such as a touchpad, microphone, keyboard, etc., where the computer **1202** is a portable computer, for example. These and other input devices are connected to the processing unit(s) **1204** through input/output (I/O) device interface(s) **1232** via the system bus **1208**, but can be connected by other interfaces such as a parallel port, IEEE 1394 serial port, a game port, a USB port, an IR interface, short-range wireless (e.g., Bluetooth) and other personal area net-

14

work (PAN) technologies, etc. The I/O device interface(s) **1232** also facilitate the use of output peripherals **1234** such as printers, audio devices, camera devices, and so on, such as a sound card and/or onboard audio processing capability.

One or more graphics interface(s) **1236** (also commonly referred to as a graphics processing unit (GPU)) provide graphics and video signals between the computer **1202** and external display(s) **1238** (e.g., LCD, plasma) and/or onboard displays **1240** (e.g., for portable computer). The graphics interface(s) **1236** can also be manufactured as part of the computer system board.

The computer **1202** can operate in a networked environment (e.g., IP-based) using logical connections via a wired/wireless communications subsystem **1242** to one or more networks and/or other computers. The other computers can include workstations, servers, routers, personal computers, microprocessor-based entertainment appliances, peer devices or other common network nodes, and typically include many or all of the elements described relative to the computer **1202**. The logical connections can include wired/wireless connectivity to a local area network (LAN), a wide area network (WAN), hotspot, and so on. LAN and WAN networking environments are commonplace in offices and companies and facilitate enterprise-wide computer networks, such as intranets, all of which may connect to a global communications network such as the Internet.

When used in a networking environment the computer **1202** connects to the network via a wired/wireless communication subsystem **1242** (e.g., a network interface adapter, onboard transceiver subsystem, etc.) to communicate with wired/wireless networks, wired/wireless printers, wired/wireless input devices **1244**, and so on. The computer **1202** can include a modem or other means for establishing communications over the network. In a networked environment, programs and data relative to the computer **1202** can be stored in the remote memory/storage device, as is associated with a distributed system. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used.

The computer **1202** is operable to communicate with wired/wireless devices or entities using the radio technologies such as the IEEE 802.xx family of standards, such as wireless devices operatively disposed in wireless communication (e.g., IEEE 802.11 over-the-air modulation techniques) with, for example, a printer, scanner, desktop and/or portable computer, personal digital assistant (PDA), communications satellite, any piece of equipment or location associated with a wirelessly detectable tag (e.g., a kiosk, news stand, restroom), and telephone. This includes at least Wi-Fi (or Wireless Fidelity) for hotspots, WiMax, and Bluetooth™ wireless technologies. Thus, the communications can be a predefined structure as with a conventional network or simply an ad hoc communication between at least two devices. Wi-Fi networks use radio technologies called IEEE 802.11x (a, b, g, etc.) to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wire networks (which use IEEE 802.3-related media and functions).

The illustrated and described aspects can be practiced in distributed computing environments where certain tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules can be located in local and/or remote storage and/or memory system.

What has been described above includes examples of the disclosed architecture. It is, of course, not possible to describe

15

every conceivable combination of components and/or methodologies, but one of ordinary skill in the art may recognize that many further combinations and permutations are possible. Accordingly, the novel architecture is intended to embrace all such alterations, modifications and variations that fall within the spirit and scope of the appended claims. Furthermore, to the extent that the term “includes” is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term “comprising” as “comprising” is interpreted when employed as a transitional word in a claim.

What is claimed is:

1. A device comprising:
computer-executable instructions; and
a hardware processor configured to execute the computer-executable instructions, wherein the computer-executable instructions cause the hardware processor to:
store, at the device, an encryption key usable to decrypt encrypted credentials, wherein the encrypted credentials are stored at a cloud framework and the encryption key is not known to the cloud framework;
process an authentication challenge request and a recognition challenge request for access to a secure destination that is separate from the cloud framework, wherein the authentication challenge request is provided by the cloud framework and the recognition challenge request is provided by the secure destination;
generate biometric data of a user responsive to both the authentication challenge request and the recognition challenge request using a single biometric sensor;
provide the biometric data to the cloud framework, wherein the cloud framework performs authentication of the biometric data;
receive the encrypted credentials and a recognition result from the cloud framework in response to the biometric data provided to the cloud framework;
decrypt the encrypted credentials using the encryption key to obtain decrypted credentials; and
obtain access to the secure destination by providing the decrypted credentials and the recognition result to the secure destination.
2. The device of claim 1, wherein the computer-executable instructions cause the hardware processor to:
prevent the biometric data from being persistently stored on the device.
3. The device of claim 1, wherein the decrypted credentials include
a username and a password.
4. The device of claim 1, wherein the computer-executable instructions cause the hardware processor to:
create the encryption key based on a master credential and domain information of the secure destination; and
create another encryption key for decrypting other encrypted credentials for another secure destination, the another encryption key being created based on both the master credential and other domain information of the another secure destination.
5. The device of claim 1, wherein the computer-executable instructions cause the hardware processor to:
prevent the encrypted credentials from being persistently stored on the device.
6. The device of claim 1, wherein the authentication challenge request corresponds to a random challenge and the recognition challenge request corresponds to a CAPTCHA (Completely Automated Public Turing test to tell Computers

16

and Humans Apart), an input for the CAPTCHA being extracted from the biometric data.

7. The device of claim 1, wherein the biometric data comprises voice data.

8. The device of claim 7, wherein the recognition challenge comprises a prompt for a user of the device to produce speech to satisfy the prompt.

9. The device of claim 8, wherein the prompt includes a word and the speech satisfies the prompt when the biometric data includes the word.

10. The device of claim 9, wherein the computer-executable instructions cause the hardware processor to:

receive a list of recognition result candidates from the cloud framework;

display the list of recognition result candidates on the device; and

receive a user selection of the recognition result from the list of recognition result candidates.

11. A method implemented utilizing a processor that executes instructions stored in a memory, the method comprising:

storing encrypted credentials of a user at a cloud service, wherein an encryption key usable to decrypt the encrypted credentials is stored at a client device associated with the user, the encryption key stored at the client device is not known to the cloud service, and, when decrypted, the encrypted credentials allow the user to access a secure destination that is separate from the cloud service;

sending an authentication challenge request from the cloud service to the client device;

receiving biometric data of the user from the client device, wherein the biometric data is responsive to both the authentication challenge request sent from the cloud service to the client device and a recognition challenge request provided by the secure destination;

authenticating the biometric data at the cloud service to obtain an authentication result responsive to the authentication challenge request sent from the cloud service to the client device;

processing the biometric data to obtain a recognition result responsive to the recognition challenge request provided by the secure destination; and

provided the authentication result indicates that the biometric data is authenticated, sending the encrypted credentials and the recognition result from the cloud service to the client device.

12. The method of claim 11, further comprising:

when the biometric data is not authenticated, not sending the encrypted credentials from the cloud service to the client device.

13. The method of claim 11, further comprising:

storing multiple different encrypted credentials for multiple different secure destinations that are separate from the cloud service; and

for the multiple different secure destinations, performing multiple different instances of the sending the authentication challenge request, the receiving, the authenticating, the processing, and the sending the encrypted credentials and the recognition result.

14. The method of claim 11, wherein the recognition challenge request is a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) and the recognition result is a response to the CAPTCHA.

15. The method of claim 14, wherein the authentication challenge is a random word challenge, the authentication

17

result is a spoken response to the random word challenge, and the recognition result is a spoken response to the CAPTCHA.

16. The method of claim **11**, further comprising:

determining whether the received biometric data was input within a predefined period of time from issuance of the authentication challenge request; and

authenticating the received biometric data only if the received biometric data was input within the predefined period of time.

17. A method performed by a computer processor, the method comprising:

storing encrypted credentials of a user at a cloud framework, wherein:

an encryption key usable to decrypt the encrypted credentials is stored at a device associated with the user and the encryption key is not known to the cloud framework, and

the encrypted credentials are associated with a login page having a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart);

sending, to the device, a CAPTCHA challenge and an authentication challenge that is separate from the CAPTCHA challenge;

receiving, from the device, a biometric challenge response to the authentication challenge and a biometric CAPTCHA response to the CAPTCHA challenge, the biometric challenge response and the biometric CAPTCHA response being captured using a single biometric sensor;

18

performing biometric verification on the biometric challenge response to determine whether the biometric challenge response matches a user biometric model associated with the user; and

when the biometric challenge response is verified to match the user biometric model:

performing recognition on the biometric CAPTCHA response to obtain recognized CAPTCHA input, and

sending the encrypted credentials and the recognized CAPTCHA input from the cloud framework to the device.

18. The method of claim **17**, further comprising:

performing recognition on the biometric challenge response to obtain response words; and

determining whether the response words match challenge words of the authentication challenge.

19. The method of claim **18**, wherein the performing recognition on the biometric CAPTCHA response and the sending the encrypted credentials and the recognized CAPTCHA input are performed when the response words match the challenge words.

20. The method of claim **17**, further comprising:

determining a type of the single biometric sensor used by the device; and

generating the authentication challenge according to the type of the single biometric sensor used by the device.

* * * * *